Privacy in the Cloud: Going Beyond the Contractarian Paradigm

Masooda N. Bashir
University of Illinois at Urbana-Champaign
1308 W. Main St.
Urbana, IL 61801, USA
+1-217-244-1139
mnb@illinois.edu

Jay P. Kesan
University of Illinois at Urbana-Champaign
504 E. Pennsylvania Ave.
Champaign, IL 61820, USA
+1-217-333-0931
kesan@illinois.edu

Carol M Hayes
University of Illinois at Urbana-Champaign
504 E. Pennsylvania Ave.
Champaign, IL 61820, USA
+1-217-333-0931
carol.mullins@gmail.com

Robert Zielinski
University of Illinois at Urbana-Champaign
1308 W. Main St.
Urbana, IL 61801, USA
+1-217-244-1139
zielins2@illinois.edu

ABSTRACT
Human life today has become entangled in the Internet. We access e-mail, store content, and use services online without a thought as to where data reside or how data are protected. The "cloud," a conceptualization of how data reside on the Internet rather than locally, is the latest technological innovation or computing trend du jour. However, many concerns surrounding cloud computing remain unaddressed. How are the data we store online kept confidential? Who else has the right to access our private information? What kind of laws and policies offer us protection?

We begin by evaluating the current situation by examining the Terms of Service (ToS) agreements and privacy policies from well-known cloud providers, and we describe the types of privacy protections (or lack thereof) that they offer. We conclude that a contractarian approach to privacy protection is likely to lead to a situation in which consumers end up trading their privacy without being well-informed about the implications and consequences of their choices.

Next, we examine whether the applicable laws are adequate to protect the privacy of consumers in the cloud. We discuss privacy protections in the cloud by considering the Fourth Amendment, the Stored Communications Act, the Federal Information Security Management Act, and the USA PATRIOT Act, and we conclude that they are inadequate in according a minimum level of privacy to consumers in the cloud, setting the stage for a vigorous study of the form and substance of cloud computing-centric privacy legislation.

Categories and Subject Descriptors

ACSAC ,Äô11 Dec. 5-9, 2011, Orlando, Florida USA

General Terms
Security, Standardization, Legal Aspects, Cloud Computing

Keywords
Cloud Computing contracts, Privacy, Legal Aspects

1. WHAT IS "CLOUD COMPUTING"?
Cloud computing as a concept is not new, but it was not until fairly recently that the term arose to describe decentralized computing. The term is used quite often but lacks a commonly agreed-upon definition. Generally, *cloud computing* refers to the use of hardware, storage, and systems software located in large datacenters worldwide (Armbrust 2009, p. 4). Applications are hosted through and accessed over the Internet instead of residing on one's own personal computer. The U.S. National Institute of Standards and Technology (NIST) describe cloud computing and its five main characteristics as follows: (1) on-demand self-service; (2) broad network access; (3) resource pooling; (4) rapid elasticity; and (5) measured service (Kerr, 2010, p. 4).

Cloud computing exists in a variety of forms. For example, when a cloud is made available in a pay-as-you-go manner to the public, it is known as a *public* cloud. Current examples of public clouds include Amazon's Elastic Compute Cloud (EC2), IBM's Blue Cloud, Sun's Cloud, Google's AppEngine, and Microsoft's Windows Azure. *Private* clouds, however, are the internal datacenters of individual businesses or organizations and are not made available to the public. NIST describes three cloud computing service models (Kerr, 2010, pp. 4-5):

- Software as a Service (SaaS): the consumer-facing level, with which most users are familiar. *SaaS* refers to the applications delivered to the user over the Internet for purposes such as e-mail, file storage, word processing, social networking, and other software programs.
- Platform as a Service (PaaS): a platform in the cloud, upon which applications can be developed and executed. PaaS allows developers to deploy applications

without having to purchase and manage underlying software and hardware.

- Infrastructure as a Service (IaaS): raw computing power and storage space on-demand. IaaS provides clients with full control of virtual machines created in the cloud on dedicated instances of servers.

Despite not fully understanding its inner workings, users are already starting to take advantage of the cloud's benefits. Nelson (2009), notes that the power of the cloud will allow "limitless flexibility, better reliability and security, enhanced collaborations, portability, and simpler devices" (pp. 71-72). Cloud computing allows its clients to cut costs and reduce the complexity of both routine computing tasks and computationally intensive problems. Scholars at the University of California at Berkeley (2009) stress that cloud computing will continue to pick up momentum, as it offers the following opportunities: "mobile interactive applications, parallel batch processing, the rise of analytics, extension of compute-intensive desktop applications, and 'earthbound' applications" (p. 7). This new technology allows for seemingly arduous tasks to be accomplished in smaller amounts of time, with less equipment and cheaper costs. Data can be accessed from any computer, anywhere in the world.

Unfortunately, due to its sudden surge in popularity, cloud computing may find itself prey to a host of security, privacy, and legal concerns. There is still no clear understanding as to how data may be used by service providers and how the data are disclosed to third parties. In the event of inaccessibility or service disruption, there is a question as to who is liable for missing data and outage costs. There is also an ever-present issue of jurisdiction. Svantesson (2010) separates two distinct cloud structures: domestic and transborder clouds. All clouds give rise to privacy issues, such as appropriate collection of data, appropriate data use, data disclosure, safe data storage, retention of data, data access, and ways of informing users about how these matters are handled. Transborder clouds bring additional jurisdictional issues and regulatory concerns.

The way in which those data privacy and legal concerns are addressed will undoubtedly be the largest obstacle to ubiquitous cloud computing use. In America, legislation and policy offer little privacy protection for data stored online. In Europe, the situation is slightly better. Worldwide, however, most popular cloud providers have privacy policies that allow them to treat customer data as they see fit with no legal consequence. Often, users are unaware that their data may be at risk on the cloud. As cloud computing evolves, it will be necessary to address several crucial weaknesses in this newest technological tour de force.

2. CURRENT PRIVACY POLICIES AND TERMS OF SERVICE (TOS) AGREEMENTS: THE CONTRACTARIAN PARADIGM AND ITS LIMITATIONS

Since technology is quickly outpacing current legal protection for data privacy , users may have a glimmer of hope: cloud providers' own privacy policy and terms of service agreements. Such documents are "omnipresent and nearly every large company relies on them to regulate use of its website and to disclose its data handling practices" (Robison, 2010, p. 1214). Unfortunately, most terms of service agreements and privacy policies offer no assurance that one's data will be kept confidential. In fact, some are striking in that they offer very little protection at all; several companies reserve in these agreements the right to manipulate user data as they please. Furthermore, although most people do not read those agreements, they may be legally bound to their terms even if they did no more than visit a website or use a certain provider's service.

Robison (2010) splits ToS agreements and privacy policies into three distinct categories that allow varying degrees of authority over a customer's data:

1. Explicit authority to access a customer's data for marketing purposes
2. Vague authority to access a customer's data for purposes beyond the primary services
3. Explicit prohibitions against accessing a customer's data for any purpose other than providing a specific service

The first, and least protective, type of service agreement allows cloud providers to access customer data for a variety of purposes, most commonly for advertising. As an example, Google uses both a master ToS agreement and a master privacy policy, both of which "apply to all of its cloud services, supplemented by smaller sub-agreements with provisions unique to each service." The master ToS states that "Google reserves the right to prescreen, review, flag, filter, modify, refuse or remove any or all content from any [Google] Service." Google's e-mail service emphasizes a similar lack of protection: "the Gmail filtering system also scans for keywords in users' e-mail which are then used to match and serve ads. When a user opens an e-mail message, computers scan the text and then instantaneously display relevant information that is matched to the text of the message" (Robison, 2010, p. 1216). In addition to enabling access to user data, Google and its partners rid themselves of any liability by services that "might be interrupted, untimely, insecure, full of errors, give inaccurate or untimely results, and have low quality" (Mowbray, 2009, p. 6). By using its services, one agrees that Google shall not be liable for "any direct, indirect, incidental, special, consequential or exemplary damages." Such sweeping ToS agreements and privacy policies are not specific to Google. Many other cloud providers disclose their intention to access customer data and use it for advertising. Evernote, an online content storage service, states that "it may display advertisements that may be targeted to content subject matter." Similarly, the social networking service Epernicus requires its users to "grant it an unrestricted license to access and use users' content for 'any purpose'" (Robison, 2010, p. 1217).

The second type of user agreement provides terms that are somewhat vague. Cloud providers, under these agreements, reserve the right to access user data, but do not specify when or for what purpose they will use it. These agreements cash in on their ambiguous nature, making it nearly impossible for users to have a precise understanding of their privacy protections. Amazon Web Services and YouTube are two examples of cloud providers that use such agreements.

On the bright side, some providers offer guidance on their intended use of user information. Yahoo! "reserves the right to 'pre-screen' content on its service, but at least for its webmail service, explains that 'Yahoo!'s practice is not to use the content of messages… for marketing purposes" (p. 1217). Although statements in these ToS agreements and privacy policies offer

some warning, they do not enable users to be fully aware of threats to their data confidentiality.

The third and final type of ToS agreement "offers customers an explicit promise not to access their data." Although not in abundance, some cloud providers assure users that their data will not be accessed when in storage on their service. Remember the Milk, a provider that offers a task management service, does not allow any authority to access a customer's data. In addition, Mozy, a cloud provider known for its automated back-up storage, asserts, "[w]e will not view the files that you backup using the Service." Unfortunately, user agreements such as these are atypical, because most cloud companies use contextual advertising in order to provide their services at little or no cost to the consumer. Popular cloud computing companies, such as Google and Amazon Web Services, are unlikely to offer more protections, both to provide cheaper services and to reduce any potential liability. It is also important to note that if these company policies do change, the provider is (most of the time) not obligated to inform the user. Google's Privacy Policy, for example, "may change from time to time, and Google does not undertake to notify users where changes take place" (Svantesson, 2010, p. 10). Many companies that provide notice to customers do so through postings on the company's website, also including a statement in the initial privacy policy reminding customers to read the privacy policy often in case it is updated.

The provisions in the current cloud contracts are not solicitous about consumer privacy. Indeed, to the extent that consumers are poorly informed about privacy issues, they are unlikely to bargain for more privacy regarding terms in their contracts. This informational asymmetry between the consumers and the cloud service providers with respect to privacy protections is significant. Unless we have well-informed parties on both sides of any transaction, any contract is unlikely to represent a well-bargained-for solution. Indeed, the informational asymmetry creates incentives for cloud service providers to act strategically and capitalize on the consumers' lack of knowledge about privacy issues in the cloud.

As a result of the limitations inherent in a purely private contracting solution to online privacy in the cloud, it is important to evaluate whether the applicable privacy-protecting laws currently on the books are adequate to serve as a well-designed baseline according an easily justified, minimum floor of privacy protections.

3. FOURTH AMENDMENT ISSUES

Under the Fourth Amendment to the United States Constitution, all persons are protected from unreasonable searches and seizures, and part of that protection is the warrant requirement under which investigators have the burden of establishing probable cause before a judicial official will issue a warrant. The most fundamental case in modern Fourth Amendment jurisprudence is Katz v. United States (389 U.S. 347 (1967)), in which the Supreme Court held that because the Fourth Amendment protects people instead of places, it was unlawful for police to bug a telephone booth without a warrant. This turns on whether the person had a "reasonable expectation of privacy." The test that arose in the cases following Katz looked at whether the person had an actual, subjective expectation of privacy, and whether society was prepared to view that expectation as reasonable.

It is not considered a search that triggers the Fourth Amendment warrant requirement if police obtain a list of phone numbers dialed by a suspect (Smith v. Maryland, 442 U.S. 735 (1979)), or if police obtain financial records that were voluntarily turned over to a third-party accountant (Couch v. United States, 409 U.S. 322 (1973)), because the suspects are not held to have a reasonable expectation of privacy in those circumstances. Many researchers have expressed concern that it may be difficult to secure Fourth Amendment protections of information in the cloud, since that information is inherently handled and processed by third parties, and it may be difficult to separate coding information (like phone numbers dialed, or Web addresses visited) from more protected content information (e.g., Zamani 2010). However, federal courts have recently acknowledged a reasonable expectation of privacy for emails of which copies were stored by an Internet service provider (United States v. Warshak, 631 F.3d 266 (6th Cir. 2010)), as well as for files stored on a password-protected website (United States v. D'Andrea, 648 F.3d 1 (1st Cir. 2011)). The Supreme Court also recently assumed, but did not conclusively determine as a matter of law, that there was a reasonable expectation of privacy in text messages, even though the messages had to be processed by a third-party wireless provider (City of Ontario v. Quon, 560 U.S. (2010)). However, though there are early indications that Fourth Amendment protections may apply to information in the cloud, there is not yet a clear legal answer.

A warrant must also provide sufficient detail about the evidence to be seized and places to be searched. The case law supports providing the protections of a warrant to closed containers. Courts and researchers have previously considered computers to be analogous to filing cabinets and similar closed containers for Fourth Amendment purposes (e.g., Zamani 2010). However, when cloud computing is being used, considering the potential overlap of on-site and off-site storage of information (Wells 2010), it is unclear which machine or set of machines would be considered the "container" such that a search would require a warrant for that machine. Another possible complication is the "plain view" exception to the warrant requirement of the Fourth Amendment, according to which any evidence not covered under the warrant may be seized if the evidence is in "plain view" when the investigator is in a place where he lawfully has a right to be (Zamani 2010). If a search began for information stored locally on a specific computer, but the computer was connected to a cloud service in which additional information was stored remotely, some have questioned whether the "plain view" exception to the warrant requirement would permit the search of the information in the cloud (Martin 2010).

Wells (2010) raises questions regarding the Fourth Amendment and its impact on cloud computing. The author states that as technology advances, the lines between the traditional sense of computing and cloud computing are "blurring." Local and remote data storage have become indistinguishable, thereby exposing limits in the Fourth Amendment's "Reasonable Expectation of Privacy" doctrine. After giving examples of cloud computing services and their similarities to desktop applications, he establishes that it is reasonable, even expected, for users to believe that their data are stored locally, when in fact they are stored on a remote server. Some applications "looks just like their desktop counterparts, pixel for pixel" (p. 233).

It seems that companies are beginning to shy away from traditional operating systems in favor of the cloud. Google, for example, has recently released Google Chrome OS, an operating

system that works exclusively with Web applications. Laptops known as "Chromebooks," made solely to access the Chrome browser, rely exclusively on online data storage and applications. While data on a local storage device are protected by the Fourth Amendment, data stored on the cloud are not. Novice or inexperienced users may be especially at risk if they are unable to distinguish between online and offline applications. In closing, Wells offers three solutions to resolve the issue: (1) attempt to distinguish online data from other records; (2) change the "reasonable expectation of privacy" doctrine, "clarifying it as not one but several standards under which cloud computing cases could fall"; and (3) overhaul the Fourth Amendment, shifting its focus from privacy to security (Wells 2010, pp. 237-240). As Web applications continue to thrive in place of the desktop, it is important to consider what kinds of protections are offered by the Fourth Amendment, particularly when online and offline applications remain so "blurred."

4. THE STORED COMMUNICATIONS ACT

In order to address privacy problems on the emerging Internet more properly, Congress enacted the Stored Communications Act (SCA) in 1986. Under the SCA, Congress aimed to regulate two primary uses of computer networks: "(1) electronic communications services (ECS) designed to handle 'data transmissions and electronic mail' and (2) remote computing services (RCS) intended to provide outsourced computer processing and data storage" (Robison 2010). These two categories and the distinctions between them determine the kind of privacy protections available to Internet users.

To qualify as an ECS, a service provider must satisfy two requirements: it must offer the user "the ability to send or receive electronic communications," and it must hold that electronic communication in "electronic storage." Electronic storage includes intermediate or temporary storage of communications incidental to transmission, and storage for the purpose of backup protection by an ECS provider (18 U.S.C.A. § 2510(17)). To qualify as an RCS, a service must satisfy different requirements. The provider must offer storage or processing services; data must be received from the customer electronically; content must be stored; and the provider cannot allow access to user content for any purpose other than storage or processing (18 U.S.C.A. § 2703(b)(2)(B)).

Although there are similar privacy protections for communications through ECS and RCS providers, RCS providers receive fewer privacy protections when compelled to disclose data by the government. The language of the statute would designate an unopened email as being in "electronic storage" and thus require a warrant in order for the government to obtain it. On the other hand, information stored with an RCS is considered to be just in "storage" and subject to disclosure upon issuance of a subpoena. Kerr (2004) observes that a provider is typically designated a provider of either ECS or RCS based on the particular information sought. Unless a provider satisfies one of those two sets of requirements, the provider's behavior as to the information in question is not regulated by the SCA. Robison (2010) notes that perhaps the Act's most significant protection is the "ability to prevent a third party from using a subpoena in a civil case to get a user's stored communications directly from an ECS or RCS provider." Several cases support this reading, relying on the fact that subpoenas from third parties pursuant to civil causes of action are not included in the enumerated exceptions under which a provider may voluntarily turn over the content of communications.

The SCA is a complicated piece of legislation that was written with privacy protections in mind based on use of the Internet in 1986. It has proven difficult to apply the SCA to modern computing practices. In Theofel v. Farey-Jones (359 F.3d 1066 (9th Cir. 2004)), the court rejected the government's reading of the SCA in favor of concluding that an ISP that stores copies of emails that had been previously opened and read was engaging in electronic storage "for backup protection," and therefore the ISP was an ECS provider as to these stored, previously opened emails. Kerr, in his article analyzing each piece of the SCA, notes that this case diverges significantly from traditional readings of the SCA.

The Theofel holding acknowledged a considerable overlap between the SCA's categories of ECS and RCS. However, the Theofel court also suggested in dicta that emails stored entirely with an RCS provider, if the user does not download copies of the emails, would not meet the threshold for "backup protection" under the ECS definitions within the SCA. This interpretation potentially limits the extent of ECS protection of webmail, even if the 9th Circuit's broad reading of the SCA is adopted. The interpretations of the SCA and responses to the holding of Theofel vary significantly across the country. Several recent cases involving webmail illustrate this. A South Carolina Court of Appeals case (Jennings v. Jennings (2010)) embraced the reasoning of Theofel, while rejecting the dicta and concluding that previously opened emails remaining on Yahoo!'s servers were stored for backup protection purposes in case the plaintiff had wanted to access them again, and thus were in "electronic storage." On the other hand, a federal district court in Illinois (United States v. Weaver (2009)) rejected this reading as it might apply to Microsoft's Hotmail webmail service, concluding that such emails were not in electronic storage and thus could be obtained by the government with a subpoena under the RCS rules.

Another recent case from the 9th Circuit, Crispin v. Audigier (2010), concluded that stored webmail (through the providers Media Temple, Facebook, and MySpace) was in "electronic storage" because it was kept for backup purposes. The Crispin court also held that Facebook and MySpace were providers of ECS with regard to private communications, and providers of RCS with regard to comments and wall postings that were visible only to a select number of readers. These services, the court reasoned, were analogous to private bulletin board systems (BBS), which courts have long recognized as being protected under the SCA. The finding that these companies qualified as RCS was in spite of the defendants' argument that Facebook and MySpace did not maintain the plaintiff's communications "solely" for the purpose of storage.

Applying the above to other areas of cloud computing, we note that the extent to which protections under the SCA will apply is a very open question. The SCA is most likely to protect webmail when the emails remain unopened. After that point, the extent of the protections (especially whether the provider is treated as a provider of ECS or RCS) will depend on whether a court applies the reasoning of Theofel. Additionally, any argument to treat webmail as an RCS will still have to overcome hurdles. Consider,

for example, Google's use of email content to target advertising at the account holder, which arguably is a use that is not "solely for the purpose of providing storage or computer processing services" (18 U.S.C.A. § 2703(b)(2)(B).

5. FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA)

Enacted in 2002, the Federal Information Security Management Act provides "a uniform regime to address the levels of risk that may arise from domestic and international sources" (Kerr, 2010, p. 11). It requires federal agencies to create programs that implement information security. In addition, FISMA "requires agency program officials, chief information officers, and inspectors general (IGs) to conduct annual reviews of the agency's information security and report the results to the Office of Management and Budget (OMB)." It also protects information used or operated by an external provider. The security requirements apply to outside sources dealing with federal information and any services provided by these sources (NIST, 2011, p. 15). OMB uses the collected data to report to Congress and provide oversight. In 2008, federal agencies "spent $6.2 billion securing the government's total information technology investment of approximately $68 billion" (FISMA, 2010).

Mandates like FISMA make agencies responsible for managing federal records and providing vital information about information systems and privacy or security threats. According to NIST (2011), "cloud providers are becoming more sensitive to legal and regulatory concerns, and may be willing to commit to store and process data in specific jurisdictions and apply required safeguards for security and privacy" (p.16). Liability and content exposure, however, remain a large concern. It may ultimately be the user's or organization's responsibility to be aware of privacy protections and keep data confidential.

6. THE USA PATRIOT ACT

Enacted in 2001, the USA PATRIOT Act includes provisions that may also impact cloud computing and the privacy protection of its users. The official title of the USA PATRIOT Act is "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001." The document gives the FBI access to any business record (including those maintained by a cloud provider), as long as a court order is issued (Gellman, 2009, p. 14). According to the United States Department of the Treasury, the purpose of the USA PATRIOT Act is to "deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and other purposes." In addition, the Act increases the government's ability to use a "National Security Letter (a form of administrative subpoena)" to obtain records. When one receives an order to disclose information, he is "highly limited in [his] ability to reveal that [he] received the order." Therefore, a user is highly unlikely to know if the government has obtained his information from a cloud provider that was storing or processing it. The USA PATRIOT Act makes it plausible for the government to access personal information and sensitive data stores on the cloud. Consequently, users who already distrust the government may be less likely to use cloud services for fear that their private data may be uncovered during an investigation.

7. JURISDICTIONAL ISSUES

To understand the privacy and legal protections available within the realm of cloud computing, one must address the issue of jurisdiction. Since users are able to access their information from virtually any location with an Internet connection, it is unclear where the data are actually being stored. For example, if someone accesses cloud information stored on a server in Europe from his home in the United States, which laws and regulations apply? There are numerous geographical considerations to take into account when addressing legal and privacy concerns in the cloud.

In their article discussing jurisdictional issues in cloud computing, Jaeger et al. (2008) describe the deciding factors in server and data center location. According to the authors, four primary considerations must be taken into account by cloud providers in choosing where to construct a data center: "(1) suitable physical space in which to construct the warehouse-sized buildings; (2) proximity to high-capacity Internet connections; (3) the abundance of affordable electricity and other energy resources; and (4) the laws, policies, and regulation of the jurisdiction" (Jensen, 2009).With those considerations in mind, it is understandable that many data centers are located in areas with sizable amounts of land, less expensive tax rates, and affordable electricity. Places such as "rural Iowa with its widespread wind power and rural Oregon and Washington with their ample hydroelectric power" exemplify these locations. Providers must also have servers located in close proximity to high-capacity Internet connections, to allow for heavy loads and high network traffic. However, due to high energy costs and impact on the environment, cloud providers are also seeking "greener" alternatives. For example, "routing traffic to a data center where it is night [when temperatures are cooler] could save energy, reducing costs and environmental impacts." It is worth mentioning the most unusual alternative: the possibility of water-based data centers. Recently referred to as "the Google Navy," this approach could not only save money and protect the environment, but also eliminate jurisdictional issues and potential risk of natural disaster.

The location of a cloud provider's data center greatly affects the way in which users are legally protected. It is unclear where a case will be tried when a cloud provider is involved. Individual jurisdictions vary in terms of cloud policy and regulation. Data centers located in the United States are vulnerable to "intelligence-gathering instruments like the USA PATRIOT Act, the Homeland Security Act, and the National Security Letters." Many policy issues come into play in different areas and have different impacts on providers. It is particularly important to note that these policies compel a cloud provider "to comply with a subpoena for a user's information without telling the user about the subpoena." To avoid the reach of these laws, providers have begun construction of data centers in locations that are not subject to them. An international banking organization, known as SWIFT, is considering a neutral country (Switzerland) as its data center, in an attempt to avoid legal complications and risks.

Legal issues raised by cloud computing, especially those involving jurisdiction, have largely remained unaddressed. Jaeger et al. (2008) stress that "the failure to create policies that adequately balance the needs of cloud providers, cloud users, and jurisdictions could have sizeable consequences on where the data centers of the future are located." Jurisdictional limitations may very well present a large obstacle to successful cloud computing. Many questions remained unanswered, such as what kind of role

the government plays, how individual and corporate user protections differ in varying locations, and, most importantly, whether a "cloud" is legally considered to be in solely one location or in every location that is part of the cloud?

8. RELEVANT DIFFERENCES FROM EUROPE

Issues of cross-border data transactions and cloud provider location are not specific to the United States. In his paper analyzing the Council of Europe's Convention on Cybercrime and its impact on cloud computing, Cristos Velasco San Martin (2009) discusses the importance and validity of jurisdictional concerns. He notes that successful data transfer will rely heavily on the strength of data protection and privacy law in a given location. European countries, for example, are known to have stringent privacy protections, whereas countries such as Mexico and Guatemala offer no such laws. Article 22 of the Council of Europe's Convention on Cybercrime (CoECC) "specifies criteria under which contracting states are obliged to assert jurisdiction over criminal offenses," the most likely of which are "(1) Offenses against the confidentiality, integrity, and availability of computer data and systems (Articles 2-6) and (2) Computer-related offenses (Articles 7-8)" (San Martin, 2009, p. 5). Complications arise because of the cloud's ability to be anywhere, at any time. Local and national laws may or may not apply, depending on the place where a crime has occurred. Unfortunately, the "cloud" is a metaphor, and its location is hard to pinpoint. Should criminals be pursued at the point of access, or at "the location of equipment, server, database, software, or website?"

The CoECC is anomalous; privacy is otherwise highly valued and protected in the EU, where a number of privacy directives have been passed. Recently, an ePrivacy Directive was passed that requires that a user's informed consent be obtained before a provider begins to store and access information that is on the user's computer. Since the EU's Data Protection Directive considers IP addresses and other unique identifiers to be personal data, this places significant restrictions on the use of cookies (Lanois 2010). The EU's Data Protection Directive also places limits on the transfer of personal data by companies to foreign countries, requiring those countries to offer adequate protection for the privacy of the information. The United States does not provide adequate privacy protections under the EU standards, but many companies in the United States obtain a Safe Harbor certification that permits them to transfer personal information from the European Union to the United States. As an alternative, cloud providers could operate segregated EU clouds for service only to EU customers.

In an age when a user can access data instantly thousands of miles from the source, protecting data privacy should not be taken lightly. Many organizations are concerned that sensitive data stored outside the country of origin may be subject to foreign government access, such as through the use of documents such as the USA PATRIOT Act. When choosing server locations, cloud providers need to be aware of the laws and policy surrounding information technology in that jurisdiction. Recently, Amazon has allowed its users to choose whether storage and processing of their data are done in Europe rather than the U.S. This option was added "partly to reduce latency for European customers, but also because of data protection issues" (Mowbray, 2009, p. 5).

9. THE WAY FORWARD

It has become increasingly clear that widespread adoption of cloud computing is inevitable. Lead technologists forecast that "within 5 to 10 years, 70% or even 90% of the world's computing and data storage will occur 'in the cloud'" (Nelson, 2009, p. 71). With that in mind, it is important to take note of the potential legal and privacy concerns that come with it.

As technology has evolved over the past few decades, and consumers continue to be poorly informed about the privacy concerns posed by these technology advances, reliance on purely contractual solutions to protect consumer privacy is likely to result only in further evisceration of individual privacy. Unfortunately, existing legislation and policies have failed to provide an important baseline regime of privacy protection. Many of the privacy protections set in place for information technologies, such as the Stored Communications Act, were established in the 1980s or 1990s and are not equipped to handle issues in the contemporary computing environment. In order to take advantage of cloud computing's raw power and potential, these pressing issues must be addressed either through new legislation or through judicial decisions as more privacy disputes in the cloud come to the fore.

However bleak it may seem, the future is not without hope. Concerns on confidentiality and data security are beginning to come to the forefront of cloud computing discussions. Governments are starting to take advantage of the cloud's processing power, and they will, in turn, play a critical role in shaping the evolution of cloud computing. Although universal standards are not possible just yet, they could help ensure consumer trust and further the adoption of cloud computing. Existing laws and regulation must be assessed in accordance with how the cloud operates, in order to ensure that newer policies do not pose barriers to the advancement of cloud computing. As for now, "we simply do not know enough about what the right set of underlying services will be, what are appropriate difference in price and quality of services, what techniques will be best for providing reliable service, and where the best engineering tradeoffs will be" (Nelson, 2009, p. 76). Once the public policy, legal, and privacy issues are debated and addressed, users will be more likely to place their trust in online services and be more willing to tap into the cloud's potential.

10. ACKNOWLEDGMENTS

This material is based on research sponsored by the Air Force Research Laboratory and the Air Force Office of Scientific Research, under agreement number FA8750-11-2-0084. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon.

11. REFERENCES

[1] Armbrust, M. 2009. Above the clouds: a Berkeley view of cloud computing. Electrical Engineering and Computer Sciences, University of California at Berkeley, Berkeley, California. http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf

[2] Gellman, R. 2009. Privacy in the clouds: risks to privacy and confidentiality from cloud computing. *Proceedings of the World Privacy Forum*.

http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf

[3] Jaegar, P., Lin, J., and Grimes, J. 2008. Cloud computing and information policy: computing in a policy cloud? *Journal of Information Technology and Politics*, 5(3). http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.156.8335&rep=rep1&type=pdf

[4] Jansen, W., and Grance, T. 2011. Guidelines on security and privacy in public cloud computing (Draft Special Publication 800-144). U.S. Department of Commerce, National Institute of Standards and Technology. Gaithersburg, MD. http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf.

[5] Kerr, J., and Teng, K. 2010. Cloud computing: legal and privacy issues. *Proceedings of the Academy of Business Disciplines Conference*. http://www.g-casa.com/conferences/vietnam/paper/JDK_CLOUDING_9_21_10_Paper-1%5B11%5D.pdf

[6] Kerr, O. 2004. A user's guide to the Stored Communications Act, and a legislator's guide to amending it. *George Washington Law Review*, 72(1208).

[7] Lanois, P. 2010. Caught in the clouds: The Web 2.0, cloud computing, and privacy? *Northwestern Journal of Technology and Intellectual Property* 9(29).

[8] Martin, T. 2010. Hey! You! Get off of my cloud: defining and protecting the metes and bounds of privacy, security, and property in cloud computing. *Journal of the Patent and Trademark Office Society*, 92(283).

[9] Mowbray, M. 2009. The fog over the grimpen mire: cloud computing and the law. *SCRIPTed*, 6(1). http://www.law.ed.ac.uk/ahrc/script-ed/vol6-1/mowbray.asp

[10] Nelson, M. R. 2009. The cloud, the crowd, and public policy. *Issues in Science and Technology*. http://cct.georgetown.edu/Nelson%20Cloud%20Article.pdf

[11] Robison, W. J. 2010. Free at what cost?: cloud computing privacy under the Stored Communications Act. *Georgetown Law Journal*, 98(4). http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID1596975_code1461162.pdf?abstractid=1596975&mirid=2

[12] San Martin, C. V. 2009. Jurisdictional aspects of cloud computing. *Proceedings of the Octopus Conference on Cooperation against Cybercrime of the Council of Europe.* http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20cristos%20cloud.pdf

[13] Svantesson, D., and Clarke, R. 2010. Privacy and consumer risks in cloud computing. *Computer Law and Security Review*, 26(4). http://epublications.bond.edu.au/cgi/viewcontent.cgi?article=1346&context=law_pubs&seiredir=1#search=%22privacy%20consumer%20risks%20cloud%20computing%22

[14] Wells, R. B. 2010. The fog of cloud computing: Fourth Amendment issues raised by the blurring of online and offline content. *University of Pennsylvania Journal of Constitutional Law*, 12(1). http://www.law.upenn.edu/journals/conlaw/articles/volume12/issue1/Wells12U.Pa.J.Const.L.223(2009).pdf

[15] Zamani, D. 2010. There's an amendment for that: A comprehensive application of Fourth Amendment jurisprudence to smart phones. *Hastings Constitutional Law Quarterly*, 38(169).